Arab J Sci Eng (2014) 39:4077–4088
DOI 10.1007/s13369-014-1077-8

RESEARCH ARTICLE - ELECTRICAL ENGINEERING

Encryption of Video Main Frames in the Field of DCT Transform Using A5/1 and W7 Stream Encryption Algorithms

Saeed Bahrami · Majid Naderi

Received: 24 June 2012 / Accepted: 31 December 2012 / Published online: 30 March 2014

Abstract Recently, creating security in multimedia systems involving video has become one of the main needs in commercial and military usages. The most important traits of video frames are simultaneousness of frames and high volume of information. Considering these features, A5/1 and W7 stream ciphers are used for video main frames in the field of selective encryption of each DCT transform coefficient.In addition, a suitable method is expressed in order to select the encryption method of DCT transform coefficients by the stream algorithms. The simulation results of MATLAB software show that this method is suitable for multimedia security in terms of both security and execution speed of the algorithm.

Keywords A5/1 · W7 · Stream cipher · Video main frames encryption · DCT transform

الخلاصة

أصبح ـفي الآونة الأخيرة تحقيق الأمن في أنظمة الوسائط المتعددة التي تنطوي على فيديو واحداً من أهم الاحتياجات الرئيسية في الاستخدامات التجارية والعسكرية. وأكثر الصفات أهمية في إطارات الفيديو هي تزامن الإطارات والحجم الكبير من المعلومات. وبأخذ هذه الخصائص بعين الاعتبار، بالإضافة إلى ذلك، تمت صياغة طريقة مناسبة من أجل اختيار طريقة التشفير لمعاملات تحويل DCT عن طريق خوارزميات تدفق. وقد أظهرت نتائج المحاكاة باستخدام برنامج "ماتلاب" (MATLAB) أن هذه الطريقة مناسبة لأمن الوسائط المتعددة من حيث الأمن وسرعة تنفيذ الخوارزمية.

S. Bahrami (✉)
Islamic Azad University, Shahrekord Branch, Shahrekord, Iran
e-mail: bahrami_saeed@elec.iust.ac.ir

M. Naderi
Cryptography and Secure Systems Laboratory, Faculty of Electrical Engineering, Iran University of Science and Technology (IUST), Tehran, Iran
e-mail: m_naderi@iust.ac.ir

1 Introduction

Nowadays, multimedia data such as images and video are expanding in telecommunications and computer networks rapidly. Due to the widespread use of multimedia data and existent threats and attacks at the communication systems, security of this data is essential [1,2].

Challenges of multimedia encryption come from three facts: First, the volume of multimedia data is very high. Second, the multimedia data are used for real-time applications and third, the variation of data needs special synchronization [3]. Consequently, the use of encryption for security imports additional computations in the processing of this information. As a result, a balance should be established between security and data synchronization [4,5]. For this purpose, fast and lightweight encryption algorithms are used in frequency conversion. Discrete cosine transform (DCT) and wavelet transform are usually used for multimedia data including video [6–8]. The most necessary and important information is available only in some of the initial coefficients in DCT transform [9]. So, frequency conversion is done and then some percentages of necessary and important coefficients are encrypted in order to reduce the volume of computations [10].

Both mentioned transforms are usually used in the process of image and video compaction. According to Fig. 1, we can perform encryption in different parts of the compaction process.

We can perform encryption after the quantization part of the compaction process. In this method, transform is first done, then transform coefficients are quantized, and finally encryption operation is performed [11,12]. In this case, Bhargava and Wang presented real-time video encryption algorithm (RVEA) [13,14]. In the RVEA method, a key sequence is used for changing randomly the sign bits of quantization coefficients.

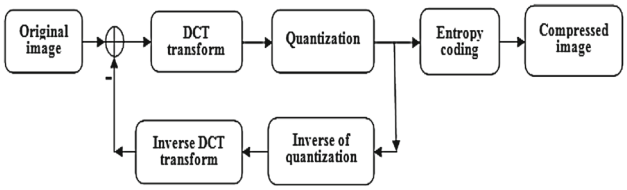

Fig. 1 Generic structure of the video compression process

Another method is the use of encryption in entropy coding part. The most commonly used coding is Huffman. In fact, this method uses Huffman tree for coding the quantization DCT coefficients. For creating security system, we can change the Huffman tree bites by using a key [15].

In this paper, A5/1 and W7 stream encryption algorithms are used following the part of quantization in the compaction process in the field of DCT transform. These algorithms have appropriate security and execution speed compared with the block encryption algorithms like DES, AES, and RC5.

2 Video Pictures

A video has been formed from a group of pictures (GOP). According to Fig. 2, each GOP in MPEG-1 coding is a series of I, P, and B pictures. I pictures are intra-frame pictures and have no relations with the other pictures. P pictures are called predictive frames that are made by using the motion vectors and also the previous I and P pictures. B pictures are bidirectional pictures that are internalized by the former and latter I or P pictures. The number of I, P, and B occurrence scan be changed with regard to the video efficiency [10,16].

Each picture is divided into several sub-blocks and each sub-block is 8 × 8 pixels (for gray scale picture). Blocks of I pictures are compacted separately, but blocks of P and B pictures are internalized with regard to the respective referential pictures and the error between the real and computed reference values. The internalization process is performed with regard to the value of the two motion vectors (the predictive forward and backward vectors) and each block in the reference picture. Figures 3 and 4 show this point. In compressing process, DCT transform, quantization, and Huffman coding are performed on each 8 × 8 block of pixels [10].

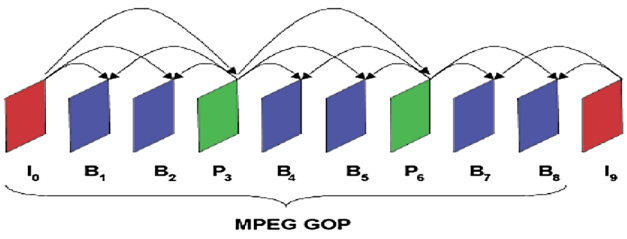

Fig. 2 A GOP including I, P, and B pictures

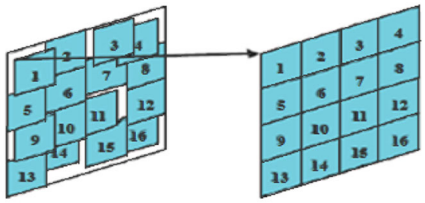

Fig. 3 Prediction by using the former reference picture

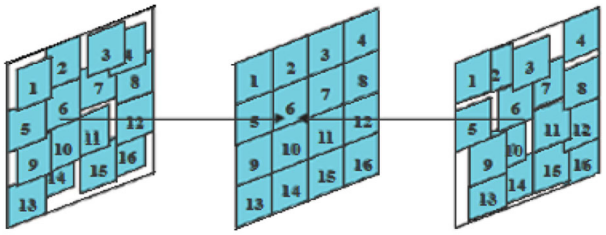

Fig. 4 Prediction by using the former and latter reference pictures

In general, there are two methods for video encoding. First, only I pictures are coded and so P and B pictures will not be easily reachable without the I picture. Second, besides the I picture, motion vectors are also coded. Of course, this method is used for military and high security usages [11].

3 DCT Transform

The discrete cosine transform (DCT) is one of the most popular transforms used in multimedia compression. It is an orthogonal transform without complex computation whose inverse can also be easily calculated. For highly correlated image data, DCT provides an efficient compaction and has the property of separability [17]. According to equation 1, DCT operates in two-dimensional condition on N by N blocks of pixels like X; its outputs are blocks with N by N blocks of pixels like Y.

$$Y_{xy} = \frac{2}{N} C_x C_y \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} X_{i,j} \cos \frac{(2i+1)x\pi}{2N} \cos \frac{(2j+1)x\pi}{2N}$$

$$\text{where } C_a = \begin{cases} \sqrt{\frac{1}{2}} a = 0 \\ 1 \quad \text{Otherwise} \end{cases} \tag{1}$$

Y is a set of N by N coefficients representing the data in the transformed domain. A set of waveforms is defined for each possible value of N (usually N = 8, thus there exist 64 waveforms). Each coefficient can be seen as the weight of each of these basic patterns or waveforms. By summing

all the waveforms scaled by the corresponding weight, the original data can be recovered [17].

4 Stream Ciphers

Stream ciphers are made by using a pseudo random key sequence which is then combined with the original text through the exclusive-or operator. Generally, stream encryption systems have suitable performance when speed and error probability of data transmission are high [18].

In general, stream encryption systems are divided into two types of simultaneous and self simultaneous ones. In the first type, the stream algorithm generates infinite sequences by selecting specific keys. The longer the frequency period of this sequence, the more apparent the properties of generated pseudo random sequences will be.

In the second type, the output sequence is built based on a function of the key and a fixed number of previous bits of the cipher text [19]. In this paper, two simultaneous stream cipher algorithms will be used that for video frames encryption are much better than any other block ciphers such as AES or DES.

4.1 A5/1 Cipher Algorithm

One of the encryption systems used in GSM mobile system is the A5/1 stream cipher. A5/1 is a simultaneous stream cipher and is built based on the linear feedback shift registers [19].

According to Fig. 5, this cipher algorithm includes 64-bit private keys and has been built from three LFSRs of 19, 22, and 23 lengths that are called R1, R2, and R3, respectively. The effective orders of R1 are in 13, 16, 17, and 18 bit positions, the effective orders of R2 in 20 and 21 bit positions, and also the effective orders of R3 in 7, 20, 21, and 22 bit positions, respectively.

The implementation key is made from the last bits of three LFSRs. LFSRs are clocked in an irregular fashion, in such a way that each time at least two LFSRs are clocked.

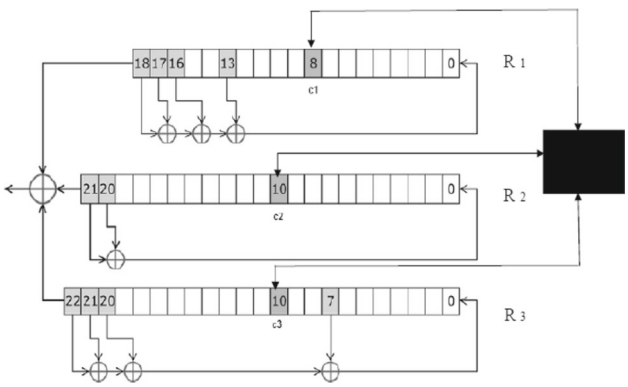

Fig. 5 The structure of A5/1 cipher

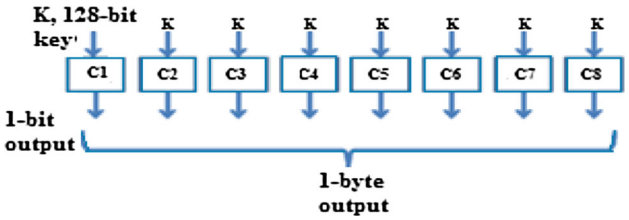

Fig. 6 The W7 key stream generator

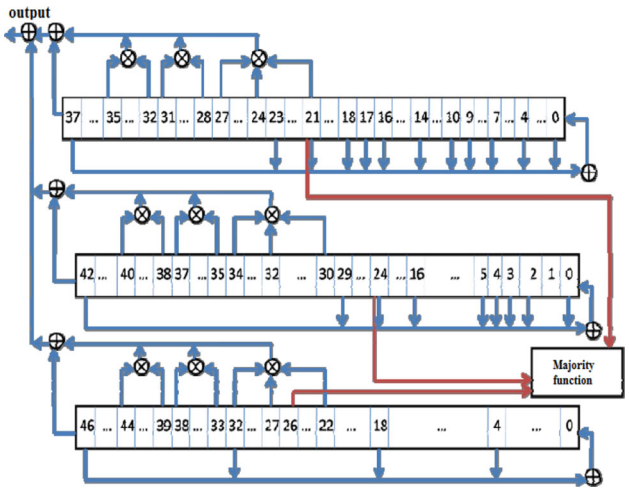

Fig. 7 Diagram of C2 block in W7 stream cipher

4.2 W7 Cipher Algorithm

W7 is a simultaneous stream cipher that is suitable for the hardware implementation and is designed for very high rates of data. This cipher has been proposed in order to replace A5/1 in GSM security plan due to the security problems in A5/1 [19].

W7 algorithm has a 128-bit key and includes a control and a function unit. The function unit consists of eight similar cells that are responsible for generating the key sequence. Each cell consists of three LFSRs and one majority function. The majority function is used to control the pulse. Figures 6 and 7 show W7 key sequence generator and the detailed plan of the C2 block, respectively. Compared with A5/1, the key length is increased from 64 to 128 bits. Each LFSR sequence is filtered by a cubic Boolean function and eight similar structures produce a byte in output instead of producing one bit.

5 Encryption of the Video Main Frames

Regarding the two mentioned stream algorithms in Sect. 3 in this article, all the performed simulations are described on the three cases of I frame from the Rhinos video, “Chemical Plant”, and “Toy Vehicle”video sequences from the USC-SIPI database with the size of 256 × 256 pixels in different modes of partial encryption of DCT transform DC

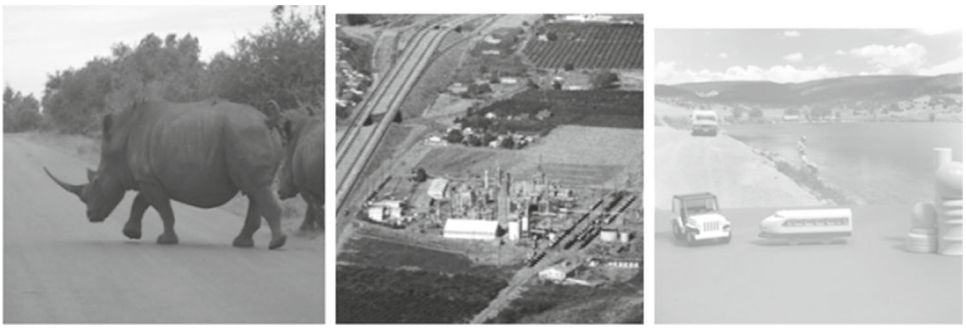

Fig. 8 Frames Rhinos (frame 10), Chemical Plant (frame5), and Toy Vehicle (frame 10) from left to the right, respectively

and AC coefficients. This database is freely available at http://sipi.usc.edu/database/. The three cases of I frame are seen in Fig. 8.

As it was mentioned in the introduction section, the security level and speed of the algorithm performance are two important parameters in video encryption and also a balance between security and synchronization is necessary. Accordingly, each one of the following cases can be used in commercial and military environments in terms of its usage.

5.1 Sign Encryption of DCT Transform

In this method, DCT transform has been done on blocks 8×8 of I frames, and then these coefficients are quantized according to MPEG compression standard matrix. The first coefficient, namely DC, has the most energy and the remaining coefficients, namely AC, have the details of the frame [14,20]. In this mode, the sign of AC coefficients is encrypted, then the inversion of both quantization and DCT transform is done, and finally the encrypted frame is depicted. The conducted process is shown in Fig. 9. It can be concluded from Fig. 9 that sign encryption of AC coefficients only reduces quality of the I frames and is utilizable for decreasing the frame resolution in commercial applications. I frame scan be recovered by statistical attacks and the cipher text-only attack in this method [11,21–23].

5.2 DC Encryption of DCT Transform

This method is similar to the previous method with the only difference that DC values are encoded instead of encryption of coefficients sign [24]. According to Fig. 10, this method is visually more secure than the previous state. This method is not secure against statistical attacks, will be more useful for commercial applications, and users cannot see the video until they do not have the cipher key.

5.3 DC and AC Encryption of DCT Transform

Regarding the point that about 75 % of AC coefficients will be equal to zero after quantification and because probability of being nonzero is more in primary coefficients, only 25 %

Fig. 9 Sign encryption. **a** The frames encrypted by the A5/1 algorithm, **b** the frames encrypted by the W7 algorithm

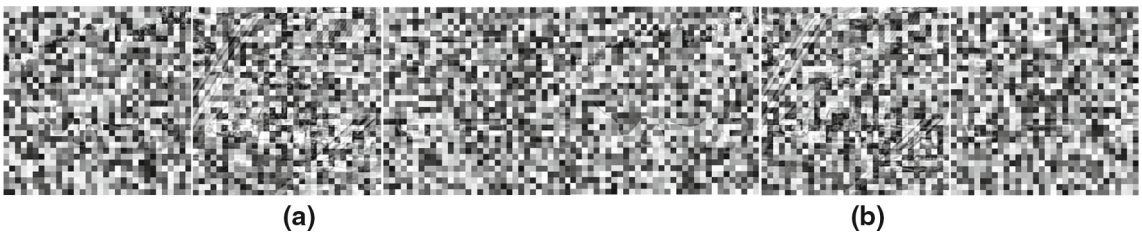

Fig. 10 Encryption of DCT transform DC coefficients. **a** The frames encrypted by the A5/1 algorithm, **b** the frames encrypted by the W7 algorithm

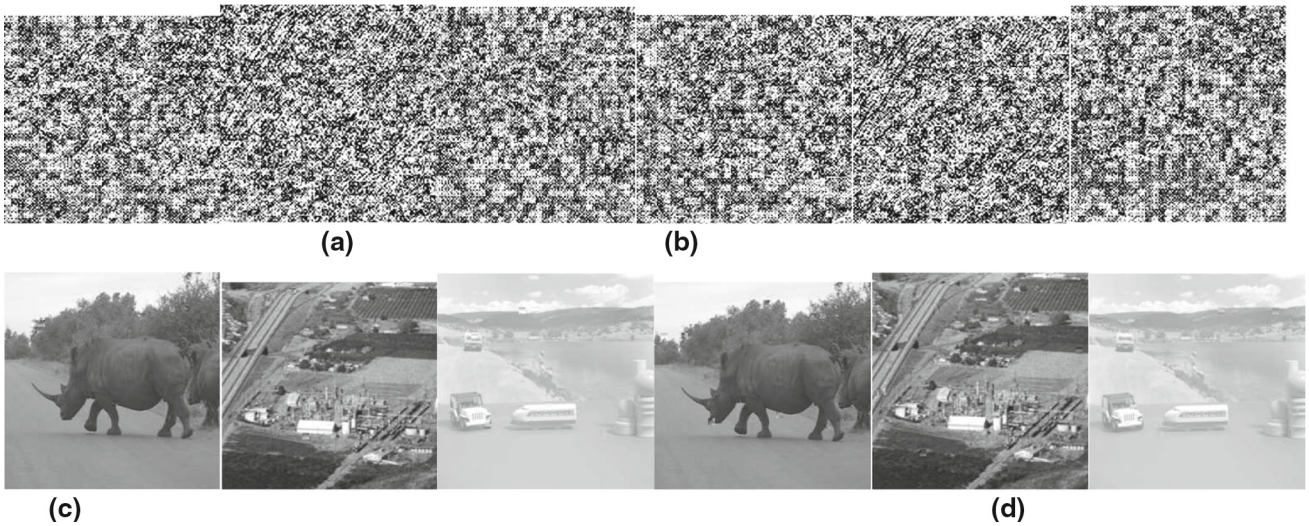

Fig. 11 Encryption and decryption of DC and AC coefficients values in the first mode. **a** The frames encrypted by the A5/1 algorithm, **b** the frames encrypted by the W7 algorithm, **c** the frames decrypted by the A5/1 algorithm, **d** the frames decrypted by the W7 algorithm

of AC primary coefficients will be encoded in this article. In addition, thanks to using the stream cipher, key sequence with plain text is logically exclusive-or, and so each coefficient can be encoded by specific numbers of bit from the key sequence. For this purpose, two suitable states, among different states, were selected with the view to security and performance speed. Four main parameters were considered in selecting these two states; First, acceptable statistical diagrams (histogram and correlation) will be obtained. Second, the least key bit will be used. Third, the acceptable peak signal to noise ratio between the encrypted frames and the decrypted ones will be obtained. Fourth, the visual quality of decryption frames will be similar to the original frames. Besides, because the primary coefficients of DCT transform have greater values than the other coefficients, more bits were used for encryption.

5.3.1 The First Mode of the Proposed Encryption Scheme

In this mode, the DC coefficient with 7-bit key and each one of the first fifteen AC coefficients with 5-bit key become logically exclusive-or. The results are shown in Fig. 11. Based on this figure, the encrypted frames have relatively high perceptual and visual security. Also, according to Fig. 11c,d, the visual quality of decryption frames is similar to the original frames.

5.3.2 The Second Mode of the Proposed Encryption Scheme

In this mode, the DC coefficient with 7-bit key and each one of the first fifteen AC coefficients with 6-bit key become logically exclusive-or. The results are shown in Fig. 12. Based on this figure, the encrypted frames have high perceptual and visual security and the visual quality of decryption frames is similar to the original frames.

5.4 The I Frame Encryption Without Transform

No transform is used in this case. A5/1 and W7 encryption algorithms are directly applied to all the pixels of I frames and any pixel is encrypted with 8-bit key by the stream ciphers. This method is more secure than the two previous modes. Figure 13a, b shows the results of the perceptual and visual encryption. The visual quality of decryption frames is plotted in Fig. 13c, d. As it can be seen, the visual quality of decryption frames is similar to the previous decryption cases.

6 The Peak Signal to Noise Ratio of the Encrypted Frames

Peak signal to noise ratio (PSNR) indicates the changes in pixel value between the encrypted picture and the original picture where the original and encrypted pictures are considered as signal and noise, respectively. It is obtained as follows:

$$\mathrm{PSNR} = 20 * \log_{10} \left[\left[\left(\frac{225}{\sqrt{\mathrm{MSE}}} \right) \right]\right] \mathrm{d}B \qquad (2)$$

where MSE is square error average and is shown as follows:

$$\mathrm{MSE} = \frac{1}{H \times W} \sum_{x=0}^{H-1} \sum_{y=0}^{W-1} |C(x, y) - P(x, y)|^2 \qquad (3)$$

where H and W are width and height of the original picture, and $P\ (x, y)$ and $C\ (x, y)$ represent the gray scale intensity

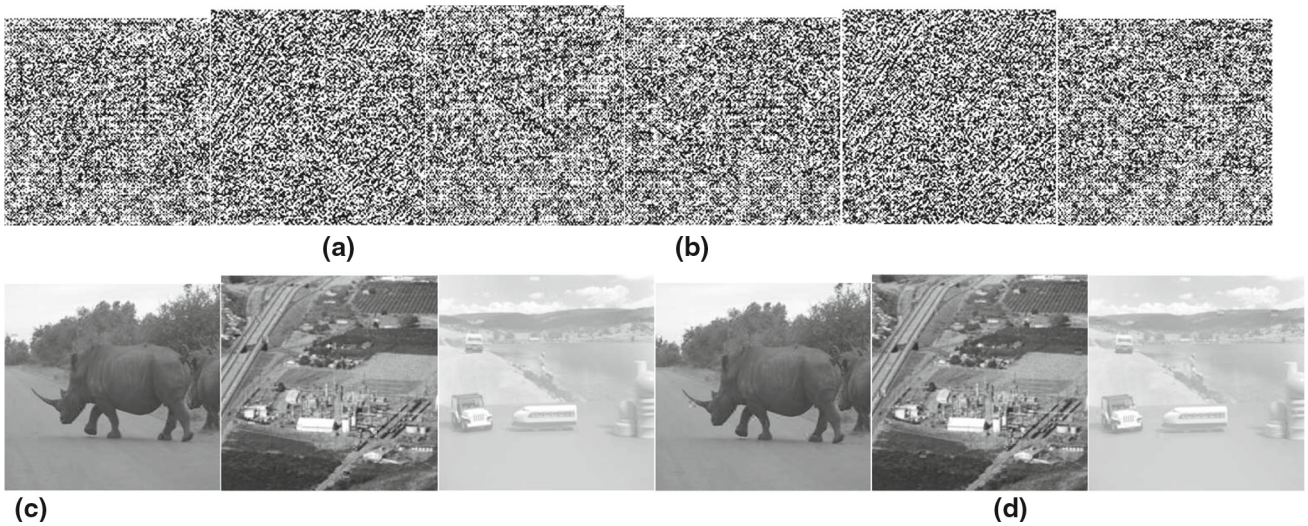

Fig. 12 Encryption and decryption of DC and AC coefficients values in the second mode. **a** The frames encrypted by the A5/1 algorithm, **b** the frames encrypted by the W7 algorithm, **c** the frames decrypted by the A5/1 algorithm, **d** the frames decrypted by the W7 algorithm

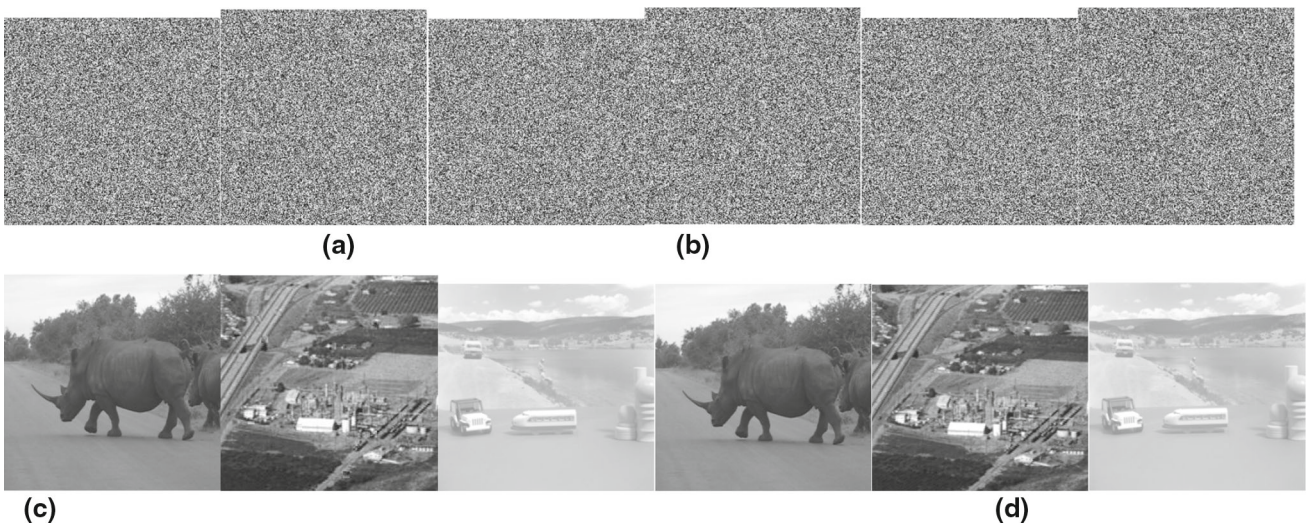

Fig. 13 Encryption and decryption without transform. **a** The frames encrypted by the A5/1 algorithm, **b** the frames encrypted by the W7 algorithm, **c** the frames decrypted by the A5/1 algorithm, **d** the frames decrypted by the W7 algorithm

of the original picture and the encrypted picture in x row and y column, respectively.

The lower PSNR values of the encrypted picture indicate the difficulty in the recovery of the original picture from the encrypted picture without having the correct decryption key [1,7,8,25]. The obtained results for different modes of A5/1 and W7 encryption algorithms as well as the different encrypted frames are available in Tables 1 and 2.

Tables 1 and 2 show that PSNR of the encrypted frames by A5/1 encryption algorithm is similar to W7 encryption algorithm. Furthermore, PSNR of encrypted frames in the DC coefficients encryption mode is higher than the other three cases. This indicates a low resistance against the cryptographic attacks than the other modes.

In addition, PSNR of encrypted frames in the two cases of the proposed encryption scheme is lower than the without transform case that shows encryption of AC and DC coefficients in the two proposed cases is appropriate for encryption of video I frames. It is notable that PSNR of the second case is lower than the first and the other cases. This shows that the second case has the highest resistance against the picture recovery attacks.

7 Histogram Analysis

To prevent the information leakage and aggressive attacks, it must be ensured that the main and encrypted frames do not

Table 1 PSNR of different encrypted frames in different encryption modes and by using A5/1 algorithm

Frame number	DC coefficients encryption	The encryption of DC and AC coefficients in first mode	The encryption of DC and AC coefficients in second mode	Without transform encryption
Rhinos (10)	8.8229	7.4639	6.7163	8.7968
Rhinos (35)	10.05	8.1587	7.2397	9.9944
Rhinos (85)	8.3514	6.9147	6.2632	8.0492
Chemical plant (10)	9.6951	7.8507	7.0393	9.1507
Toy vehicle (5)	7.9294	6.7762	6.1988	7.8638

Table 2 PSNR of different encrypted frames in different encryption modes and by using W7 algorithm

Frame number	DC coefficients encryption	The encryption of DC and AC coefficients in first mode	The encryption of DC and AC coefficients in second mode	Without transform encryption
Rhinos (10)	8.8011	7.4372	6.6396	8.5230
Rhinos (35)	10.0080	8.2123	7.2282	10.0001
Rhinos (85)	8.3475	6.8088	6.1787	8.0913
Chemical plant (10)	9.6123	7.9115	6.9955	9.1634
Toy vehicle (5)	7.9091	6.8237	6.1424	7.9041

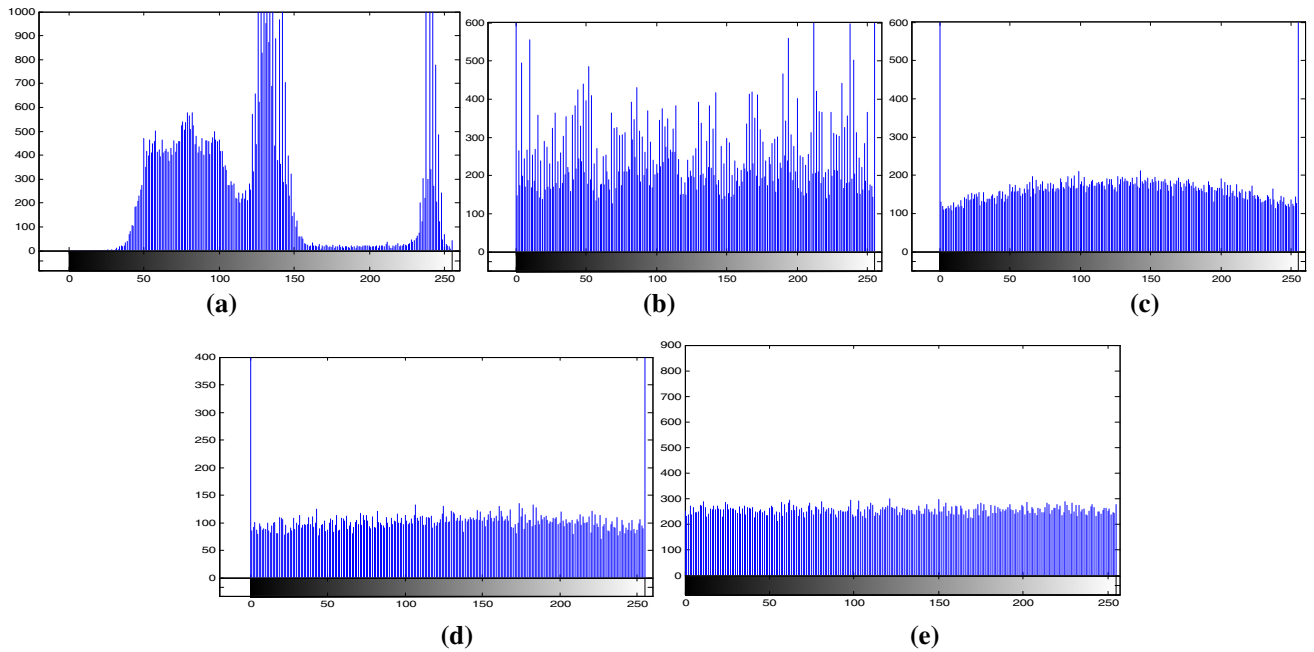

Fig. 14 Histogram graphs of A5/1 encryption algorithm. **a** Frame 10 of Rhinos video, **b** encryption of DC coefficients, **c** encryption of DC and AC coefficients in the first mode, **d** encryption of DC and AC coefficients in the second mode, and **e** encryption without transform

have any statistical similarities. Histogram analysis expresses the way of the distribution of pixels in main frame using the drawing number of observations for each amount of pixels brightness [5,9,26–28]. Uniform distribution of histogram diagram could indicate good quality of the encrypted picture.

Figures 14 and 15 show histogram of the main and encrypted frames. As you can see, histogram of both the two mentioned states of DC and AC coefficients encryption has no statistical similarity to histogram of the original frames. Therefore, statistical attacks are not efficient based on these graphs and only histogram of the second state in smoother

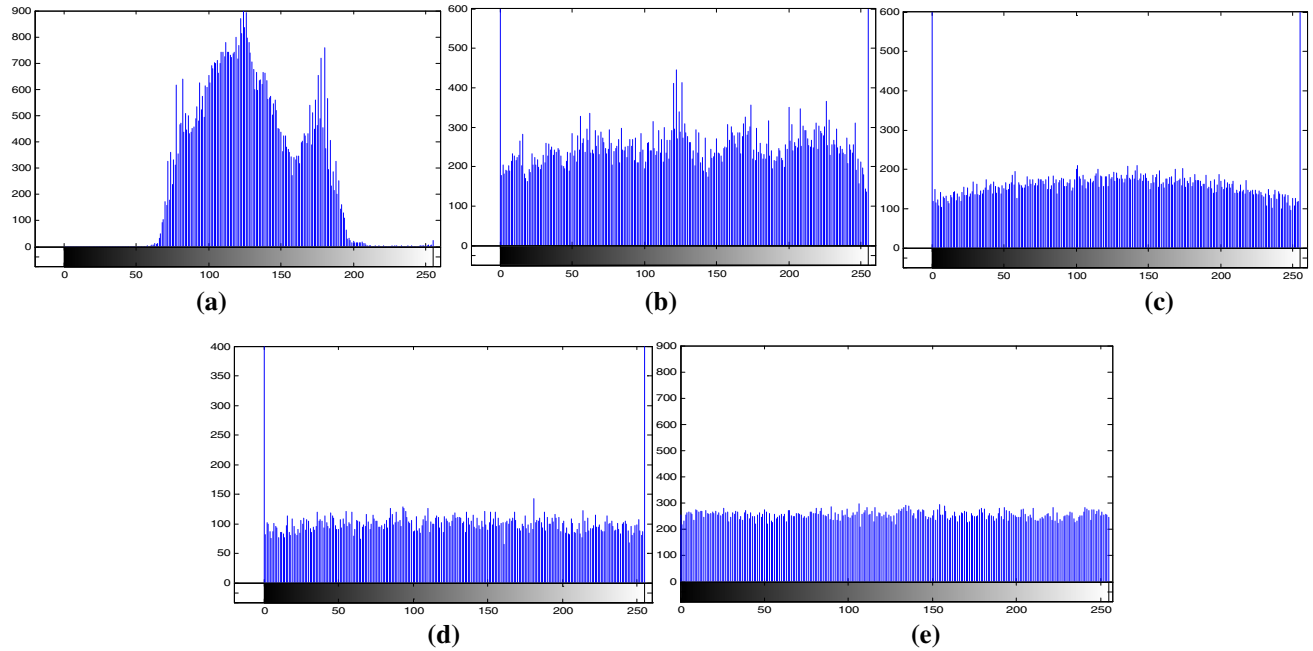

Fig. 15 Histogram graphs of W7 encryption algorithm. **a** Frame 35 of Rhinos video, **b** encryption of DC coefficients, **c** encryption of DC and AC coefficients in the first mode, **d** encryption of DC and AC coefficients in the second mode, and **e** encryption without transform

than the first state. In addition, with regard to histogram uniform distribution of without transform state and the second state of DC and AC coefficients encryption, it is concluded that A5/1 and W7 algorithms are secure against statistical attacks.

8 Correlation Analysis

In the main picture, any pixel is highly correlated with its neighboring pixels. An ideal encryption algorithm must produce encoded pictures with less correlation among its pixels. For this purpose, the correlation diagram is used. For drawing this diagram, 1,000 pairs of two adjacent pixels are selected randomly from picture and horizontal, vertical and diagonal neighborhood of N pixels is identified. Then, diagram is plotted based on the value of each pixel and its neighbors [9,26–28].

According to Figs. 16 and 17, because there is too much correlation among pixels in the main frames, correlation diagrams are seen linearly, but in the suitable and acceptable cryptography the linear mode is not shown because the correlation between pixels decreases sharply.

As it is shown in Figs. 16 and 17, correlation diagrams of encrypted frames are seen linearly in DC coefficients encryption mode. This indicates a low resistance against cryptographic attacks than the other modes. Besides, the correlation diagram of pixels in the second mode of DC and AC coefficients encryption is more dispersed from the first mode of DC and AC coefficients encryption. Therefore, the second mode is more secure against statistical attacks than the first mode. In addition, with regard to the correlation diagrams of without transform state, we can conclude that A5/1 and W7 algorithms are secure against statistical attacks.

9 Performance Analysis

Apart from the security issues, the speed of implementing encryption algorithm is important for real-time processing. For demonstrating the effective implementation of cryptographic systems, an explicit comparison must be conducted between the speed of the studied encryption systems.

Efficiency of A5/1 and W7 encryption algorithms and the different modes in the field of transform and without transform has earned with a MATLAB code on a machine with Intel core 2 Duo 2.10 processor and 2 GB of RAM memory for Windows7 operating system and gray scale images with 256×256 pixel dimensions. References [1,3,5,8,10,28,29] have given the run times of their algorithm just to compare the speed of execution according to their performance conditions. Therefore, the run times of two algorithms in different modes are given in this article to compare the speed of execution in Tables 3 and 4.

Based on Tables 3 and 4, the results show A5/1 stream algorithm is faster than W7 stream algorithm. Therefore, the A5/1 stream algorithm for real-time multimedia applications is more appropriate than W7 stream algorithm. Meanwhile,

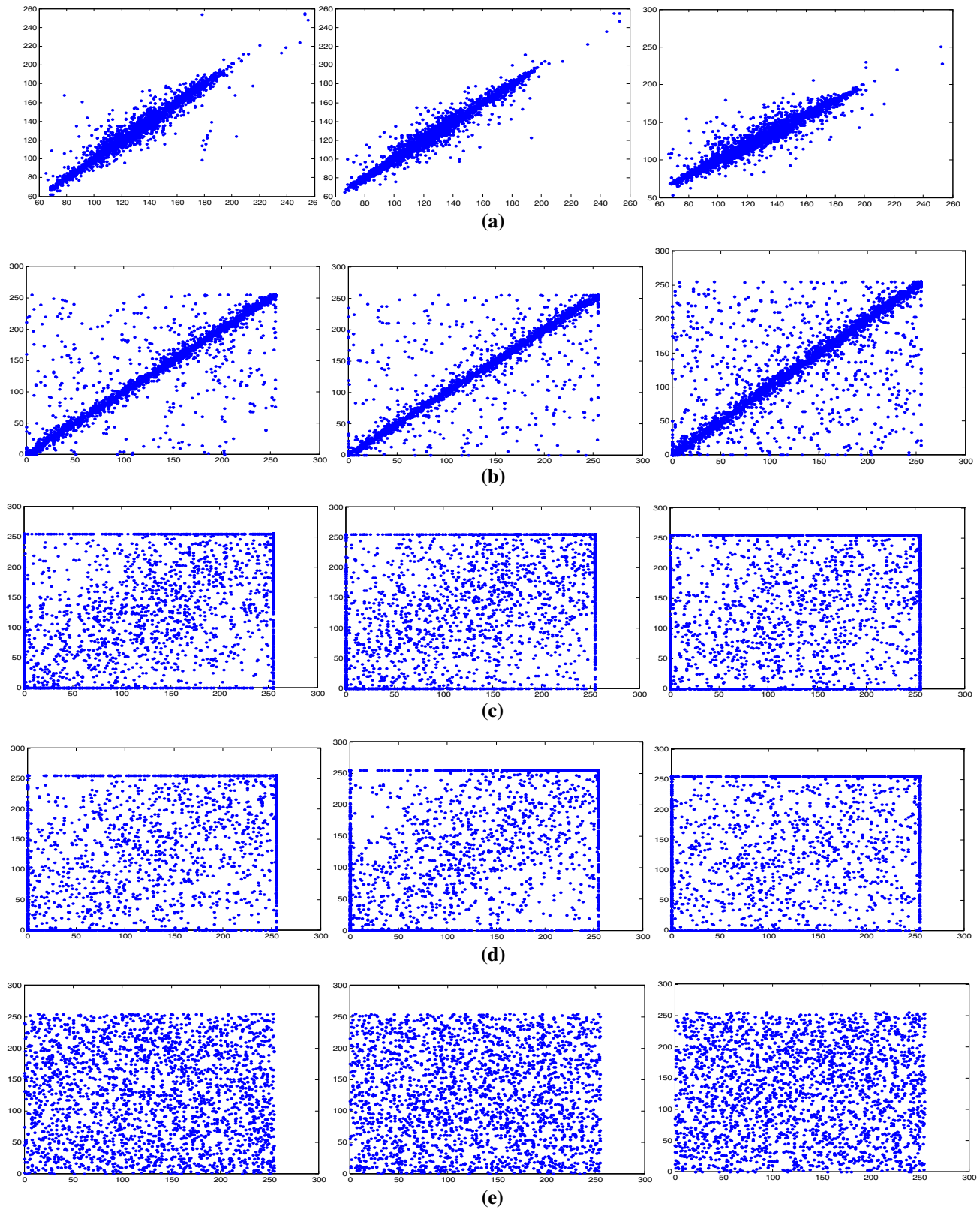

Fig. 16 Correlation chart of A5/1 encryption algorithm. *Leftside* with neighborhood of horizontal, *center* with neighborhood of vertical, *rightside* with neighborhood of diagonal. **a** Frame 35 of Rhinos video, **b** encryption of DC coefficients, **c** encryption of DC and AC coefficients in the first mode, **d** encryption of DC and AC coefficients in the second mode, and **e** encryption without transform

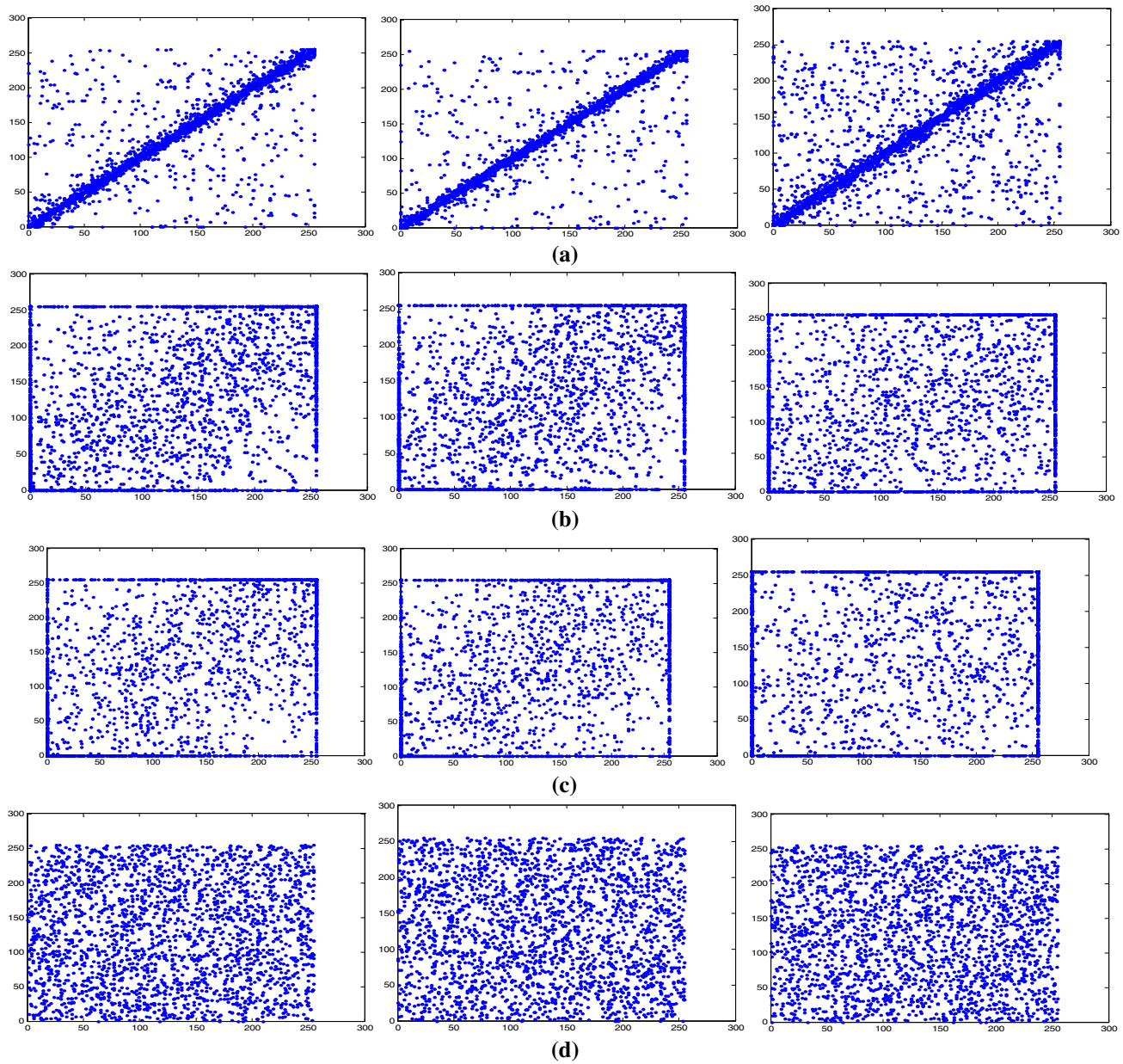

Fig. 17 Correlation chart of W7 encryption algorithm. *Leftside* with neighborhood of horizontal, *center* with neighborhood of vertical, *rightside* with neighborhood of diagonal. **a** Encryption of DC coefficients, **b** encryption of DC and AC coefficients in the first mode, **c** encryption of DC and AC coefficients in the second mode, and **d** encryption without transform

Table 3 The executive analysis of encrypted different frames in different encryption modes and by using A5/1 algorithm (second)

Frame number	DC coefficients encryption	The encryption of DC and AC coefficients in first mode	The encryption of DC and AC coefficients in second mode	Encryption without transform
Rhinos (10)	0.6326	1.9630	2.2781	10.3054
Rhinos (35)	0.6323	1.9565	2.2574	10.2272
Rhinos (85)	0.6362	1.9662	2.2459	10.3507
Chemical plant (10)	0.6351	1.9651	2.2578	10.2154
Toy vehicle (5)	0.6361	1.9621	2.2621	10.3149

Table 4 The executive analysis of encrypted different frames in different encryption modes and by using W7 algorithm (second)

Frame number	DC coefficients encryption	The encryption of DC and AC coefficients in first mode	The encryption of DC and AC coefficients in second mode	Encryption without transform
Rhinos (10)	0.9754	4.7808	6.9623	27.4552
Rhinos (35)	0.9670	4.6424	6.9554	28.2145
Rhinos (85)	0.9581	4.5551	7.0112	27.7882
Chemical plant (10)	0.9548	4.5891	7.0124	27.9187
Toy vehicle (5)	0.9701	4.7145	6.9871	28.3651

we can conclude that the execution times of the without transform mode are greatly more than the DC coefficient encryption as well as the two proposed modes of DC and AC coefficients encryption. Although DCT transform computation and its inverse increase the run time, reduction in run times of the transform cases compared with the without transform case is due to the fact that just some of the initial and necessary coefficients are encoded. Thus,the total execution time in the selective coefficients encryption mode has been obtained less than the one in the case of encryption of all the pixels. On the other hand, the execution times of the two algorithms in the two proposed modes will be useful just for I frames and are not efficient for P and B motion frames. In addition, it is worth mentioning that these times are relative and using processors with more processing speed can decrease these values significantly.

10 Conclusion

The present article proposes the multimedia networks security with regard to synchronization challenges and high volume of data. Video data differ from common data in terms of synchronization and large volume of information. If we want to use cryptography for securing these kinds of data, additional computations will be necessary for processing this information. Therefore, a balance must be made between security and synchronization. For obtaining these goals, secure and simple stream algorithms were used in DCT transform domain by partial encryption of transform coefficients and also cryptography of the video main frames. Each one of these parameters was set and regulated based on commercial or military applications. In addition, a suitable method was proposed by stream algorithms for selecting the way of cryptography of each DCT transform coefficient. Based on histogram and correlation statistical diagrams and also the peak signal to noise of the encrypted pictures, it can be concluded that the security of this method is comparable with the without transform state, and also it is minimally three times as much as the without transform state in the light of the speed of the algorithm implementation that is very important for video real-time application.

References

1. Taneja, N.; Raman, B.; Gupta, I.: Combinational domain encryption for still visual data. Multimed. Tools Appl. **59**(3), 775–793 (2012)
2. Uhl, A.; Pommer, A.: Application scenarios for the encryption of still visual data. In: Image and video encryption from Digital Rights Management to secured personal communication. Advances in Information Security, vol. **15**, pp. 31–43. Springer, Berlin (2005)
3. Agaian, S.S.; Rudraraju, R.G.R.; Cherukuri, R.C.: Logical transform based encryption for multimedia systems. In: IEEE International Conference on System Man and Cybernetics (SMC), pp. 1953–1957 (2010)
4. Bao, F.; Deng, R.H.: Light-weight encryption schemes for multimedia data and high-speed networks. In: IEEE Global Telecommunications Conference, pp. 188–192 (2007)
5. Bahrami, S.; Naderi, M.: Image encryption using a lightweight stream encryption algorithm. In: Advances in Multimedia, the Journal Special Issue for Web Services in Multimedia Communication, vol. **2012**. Article ID 767364 (2012)
6. Zhou, Y.; Panetta, K.; Agaian, S.: Image encryption using discrete parametric cosine transform. In: Forty-Third Asilomar Conference on Signals, Systems and Computers, pp. 395–399 (2009)
7. Seo, Y.-H.; Choi, H.-J.; Kim, D.-W.: Digital hologram encryption using discrete wavelet packet transform. Opt. Commun. **282**(3), 367–377 (2009)
8. He, X.; Zhang, Q.: Image encryption based on chaotic modulation of wavelet coefficients. In: IEEE Computer Society, Congress on Image and Signal Processing, pp. 622–626 (2008)
9. Krikor, L.; Baba, S.; Arif, T.; Shaadan, Z.: Image encryption using DCT and stream cipher. Eur. J. Sci. Res. **22**(1), 47–57 (2009)
10. Raju, C.N.; Umadevi, G.; Srinathan, K.; Jawahar, C.V.: Fast and secure real-time video encryption. In: Conference on Computer Vision Graphics and Image Processing, pp. 257–264 (2008)
11. Liu, F.; Koenig, H.: A survey of video encryption algorithms. J. Comput. Secur. **29**(1), 3–15 (2010)
12. Lian, S.; Chen, X.: On the design of partial encryption scheme for multimedia content. Mathematical and Computer Modelling. Available Online 16 June 2011
13. Bhargava, B.; Shi, C.; Wang, S.Y.: MPEG video encryption algorithms. J. Multimed. Tools Appl. **24**(1), 57–79 (2004)

14. Shi, C.; Bhargava, B.: A fast MPEG video encryption algorithm. In: The Sixth ACM International Conference on Multimedia, pp. 81–88 (1998)
15. Zhou, J.; Liang, Z.; Chen, Y.; Au, O.C.: Security analysis of multimedia encryption schemes based on multiple Huffman table. IEEE Signal Process. Lett. **14**(3), 201–204 (2007)
16. Massoudi, A.; Lefebvre, F.; De Vleeschouwer, C.; Macq, B.; Quisquater, J.-J.: Overview on selective encryption of image and video: challenges and perspectives. EURASIP Journal on Information Security, Hindawi Publishing Corporation. Article ID 179290 (2008)
17. Dufourny, M.C.: MPEG-4 style object-based codec with Matlab. TFE Department, Umea University, Sweden (2006)
18. Ahmed, H.E.H.; Kalash, H.M.; Farag Allah, O.S.: Encryption quality analysis of the RC5 block cipher algorithm for digital images. J. Opt. Eng, **45**(10), 277–284 (2006)
19. Jolfaei, A.; Mirghadri, A.: Survey: image encryption using A5/1 and W7. J. Comput. **2**(8), 12–17 (2010)
20. Potdar, U.; Talele, K.T.; Gandhe, S.T.: Comparison of MPEG video encryption algorithms. In: International Conference on Advances in Computing, Communication and Control (ICAC3'09), pp. 289–294 (2009)
21. Lian, S.: Multimedia Content Encryption: Techniques and Applications. Auerbach Publication, New York (2008)
22. Thomas, N.; Redmill, D.; Bull, D. Secure transcoders for single layer video data. J. Signal Process. Image Commun. **25**(3), 196–207 (2010)
23. Said, A.: Measuring the strength of partial encryption schemes. In: Proceedings of IEEE International Conference on Image processing, ICIP 2005, vol. **2**, pp. 1126–1129 (2005)
24. Wu, C.-P.; Jay K.C.-C.: Design of integrated multimedia compression and encryption systems. IEEE Trans. Multimed. **7**(5), 828–839 (2005)
25. El-Iskandarani, M.A.; Darwish, S.; Abuguba, S.M.: A robust and secure scheme for image transmission over wireless channels. In: ICCST, pp. 51–55 (2008)
26. Li, W.; Yu, N.: A robust chaos-based image encryption scheme. In: IEEE International Conference on Multimedia and Expo, pp. 1034–1037 (2009)
27. Luo, R.C.; Chung, L.Y.; Lien, C.H.: A novel symmetric cryptography based on the hybrid haar wavelets encoderand chaotic masking scheme. IEEE Trans. Ind. Electr. **49**(4), 933–944 (2002)
28. Chen, G.; Mao, Y.; Chui, C.: A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos Solitons Fractals **12**(3), 749–761 (2004)
29. Jolfaei, A.; Mirghadri, A.: Survey: image encryption using Salsa20. IJCSI **7**(5), 213–220 (2010)